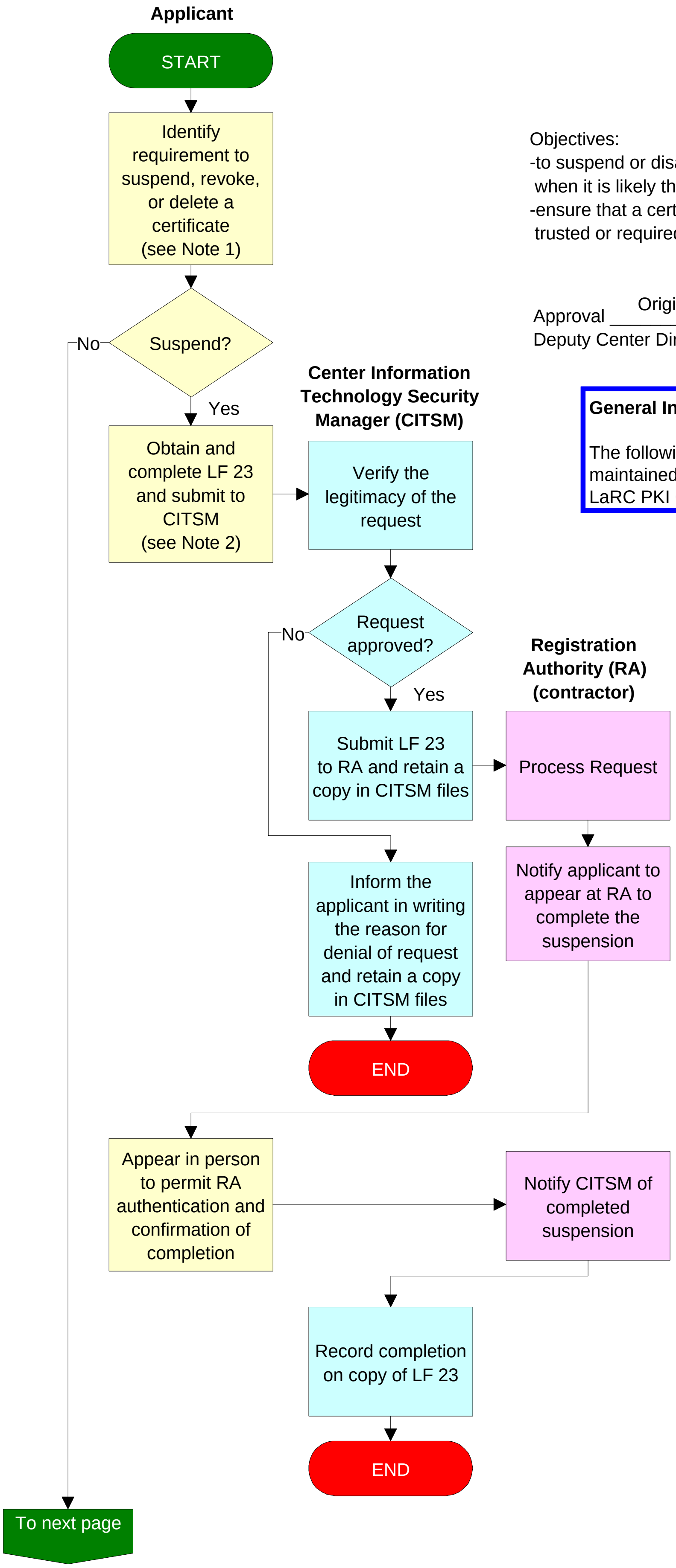
SUSPENDING OR REVOKING A PUBLIC KEY INFRASTRUCTURE (PKI) CERTIFICATE

LMS-CP-5631
Revision: A-3

Objectives:
-to suspend or disable a certificate on a temporary basis, when it is likely that the certificate may be re-enabled
-ensure that a certificate is revoked when it is no longer trusted or required for any reason

Approval ___Original signed on file___
Deputy Center Director


Applicant
START
Identify requirement to suspend, revoke, or delete a certificate (see Note 1)
Suspend?
No
Yes
Obtain and complete LF 23 and submit to CITSM (see Note 2)
Center Information Technology Security Manager (CITSM)
Verify the legitimacy of the request
Request approved?
No
Yes
Submit LF 23 to RA and retain a copy in CITSM files
Registration Authority (RA) (contractor)
Process Request
Notify applicant to appear at RA to complete the suspension
Inform the applicant in writing the reason for denial of request and retain a copy in CITSM files
END
Appear in person to permit RA authentication and confirmation of completion
Notify CITSM of completed suspension
Record completion on copy of LF 23
END
To next page

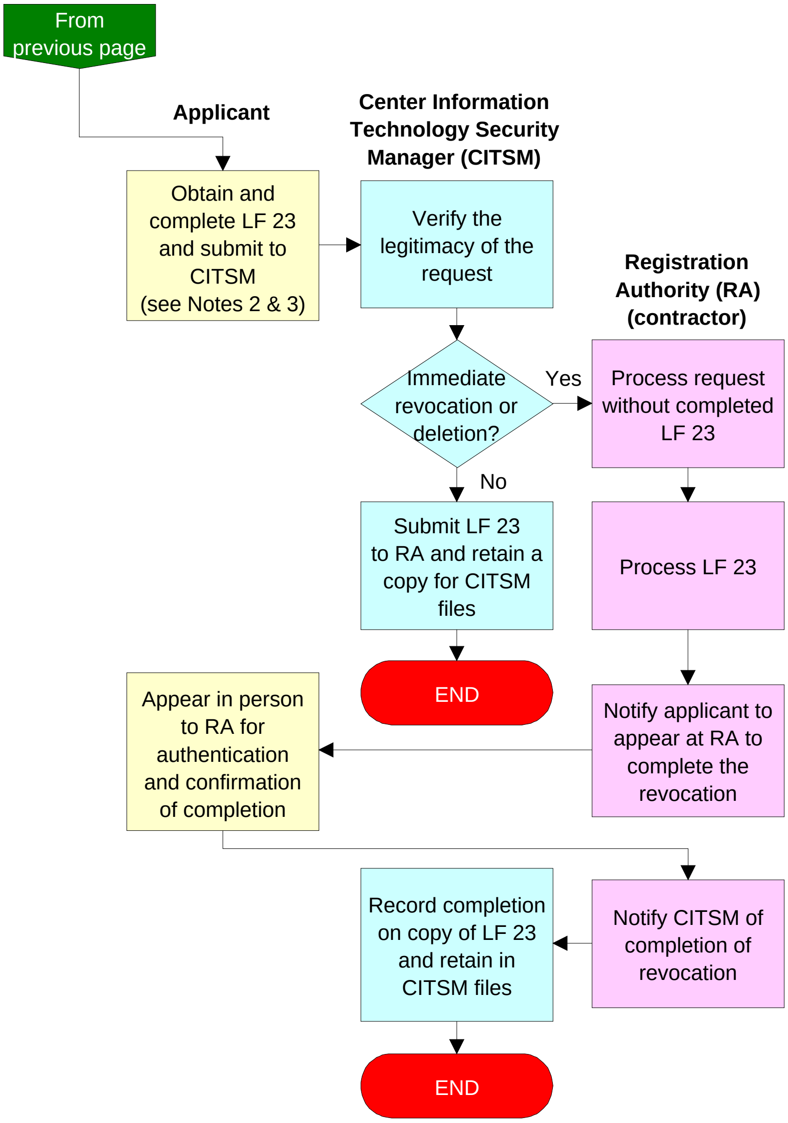
General Information

The following records are generated by this procedure and should be maintained in accordance with CID 1440.7:
LaRC PKI Certificate Suspend/Disable and Revocation Request, LF 23

Note 1
A certificate may be suspended or disabled on a temporary basis if the certificate owner will be absent for an extended period of time, but it can be re-enabled at a later date using LMS-CP-5630, "Requesting, Modifying, or Restoring a Public Key Infrastructure (PKI) Certificate"

A certificate must be revoked or deleted when it is no longer trusted. Loss of trust includes, but is not limited to:
-Dismissal or suspension for cause
-Compromise or suspected compromise of the private key, user password or profile
-Change in the certificate owner's role or permissions
-Termination of employment
-Failure of certificate owner to meet obligations specified for NASA PKI practices

Note 2
Read "What You Need to Know About Certificate Revocation and Suspension" on LF 23


From previous page
Applicant
Center Information Technology Security Manager (CITSM)
Registration Authority (RA) (contractor)
Obtain and complete LF 23 and submit to CITSM (see Notes 2 & 3)
Verify the legitimacy of the request
Immediate revocation or deletion?
Yes
No
Process request without completed LF 23
Submit LF 23 to RA and retain a copy for CITSM files
Process LF 23
END
Appear in person to RA for authentication and confirmation of completion
Notify applicant to appear at RA to complete the revocation
Notify CITSM of completion of revocation
Record completion on copy of LF 23 and retain in CITSM files
END

Note 3
For compromise or suspected compromise of a private key and dismissal for cause, the CITSM must be notified within 1 hour for immediate revocation of user access. This is classified as an IT security incident. Follow up with a completed LF 23. The CITSM will coordinate with the RA for immediate revocation. If the CITSM is not available, contact the RA directly.

For all other revocations, the CITSM must be notified within 24 hours with a completed LF 23.